datastring

CLOUD BACKUP

Frequently Asked Questions

datastring

1 Installation

2 Setup of Backup Sets and Schedules

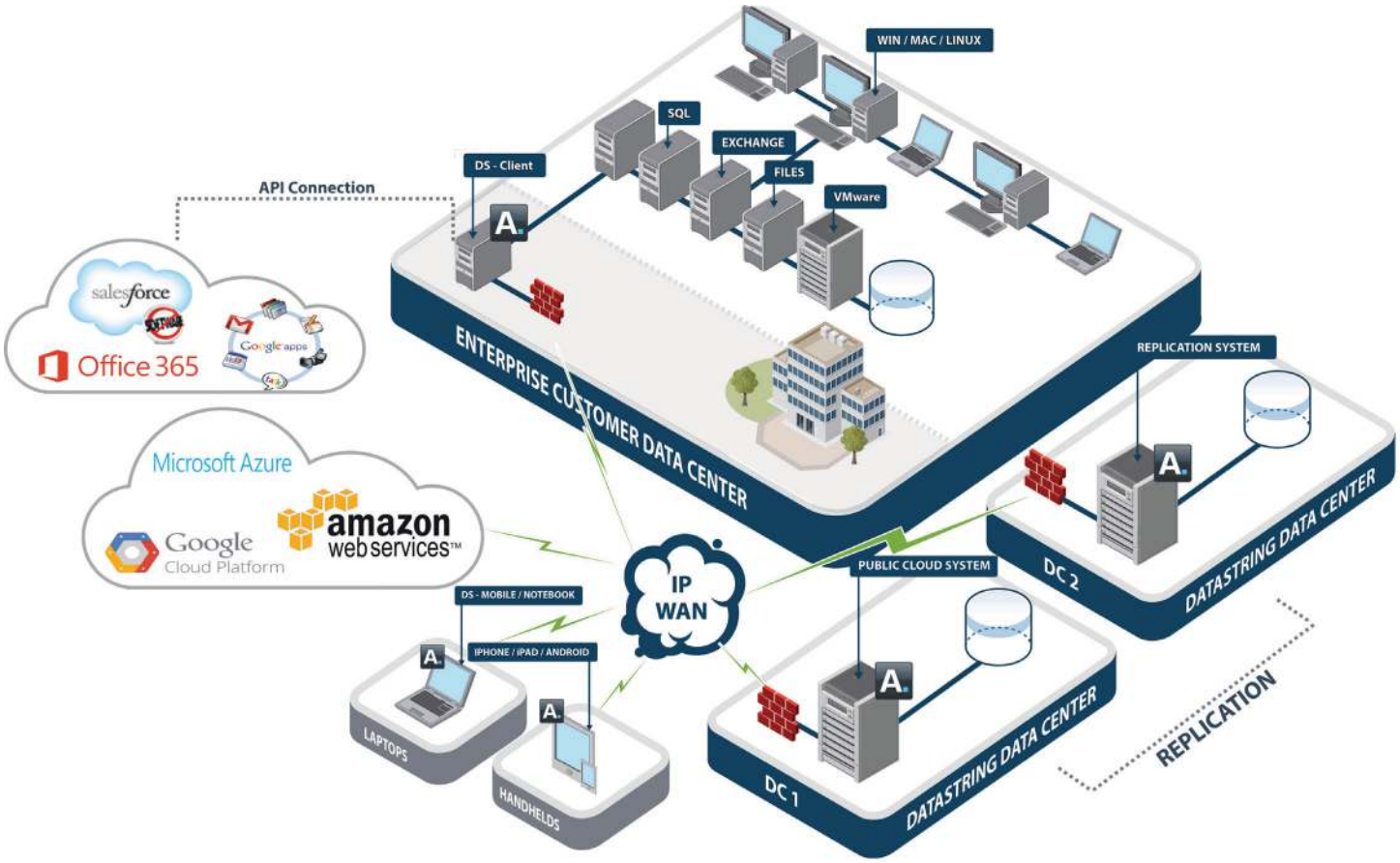
3 Data Processing & DS-Client

4 Monitoring

5 Compression, Encryption and Security

11 Data Protection

12 Virtualization



Installation

1.1 Is software installed on any other machines at the site that we are backing up?

Only two pieces of software are installed on the customer's LAN either on the source machine or on separate machines: DS-Client that collects data and sends it to the Datastring Data Center, and DS- User that acts as the user GUI and enables configuration of all backups and restores.

1.2 How is the DS-Client connected to our network?

Datastring DS-Client has one network connection to your network and one connection to Datastring's network/internet (with access to the Datastring's DS-System). This flexible approach allows Datastring to integrate fully with your current configuration.

1.3 Who installs the Datastring service?

Datastring will assist with the installation of the DS-Client unit and the DS-User Console at your site and provide the necessary training. If the installation is particularly complex or remote sites are involved, onsite support is available at a daily rate.

1.4 Can DS-Client be installed through RDP?

Installation of Datastring software can be done through a Remote Desktop Connection. Once installed, DS-Client can be managed through a remote session or can be managed through a DS-User GUI installed remotely.

Setup of Backup Sets and Schedules

2.1 What access permissions does the backup user require?

The backup user is responsible for backing up and restoring all the data on your network, it is essential that access permissions are of administrative equivalence. Datastring can only back up data that this user can access. A less privileged user may be restricted, causing data to be missed from the backup.

2.2 Who is authorized to use the DS-User GUI?

Customers can set up users with access to create and maintain backup sets and schedules. Only people with a user ID on the DS-Client or on the Domain it belongs to will be able to administer its functions.

2.3 Can users administer backups for their own machines?

Multiple user accounts can be created for use on the DS-Client and access permissions can be set per backup set. These permissions can be any combination of Backup, Restore, Delete or Modify privileges. For Example, a particular user could be given access to backup and restore only their own machine.

2.4 What frequency of backup can be set?

Backups can be time-based and configured as often as every minute or as infrequently as once a year. More advanced schedule options include the last working day of the month or even one off backups on a particular date. Backups can also be triggered based on events. Continuous Data Protection (CDP) captures each change to a file regardless of the time interval.

2.5 What level of granularity is possible in setting up the backup, i.e. file level/individual database?

A backup set can include a whole server, share/volume, directory or even a single file. The backup set could even include just the registry.

2.6 Can one machine be prioritized over another?

There are 99 different priority levels that can be assigned, ensuring maximum flexibility when organizing your backup schedules.

2.7 Can multiple machines be backed up simultaneously?

Any number of machines can be backed up simultaneously. However, as network bandwidth is a factor, Datastring would recommend 8 at once in a LAN environment with a 32- bit DS-Client and 12 at once in a LAN with a 64-bit DS-Client (default values for a DS-Client installation).

2.8 Can the software be set to stop backing up a certain time has elapsed?

Yes, the software is designed to fit specific backup windows. Datastring can be told what time to stop at, for example at 8:00am when employees are starting their workday, or maybe at 5:00am if there is an important batch process to run.

Data Processing & DS-Client

3.1 If Datastring is agentless, how does it access our data?

The DS-Client uses standard APIs to capture requested data within the LAN. Therefore, the nodes to be backed up are Agentless since the DS-Client interfaces directly with all supported platforms and application through APIs.

3.2 Is data held on the DS-Client or does it pass straight through?

The DS-Client acts as a gateway only, passing data through after it has been compressed, de-duplicated and encrypted. A database showing information on what has been backed up is held on the DS-Client, but no actual data files are retained. Alternatively a local storage can be configured on DS-Client LAN. In this case, backup data is also held locally.

3.3 How is the first backup done, given that will be a lot of data?

For large data volumes, the initial backup may be done utilizing a portable unit, backing up at LAN speeds to a large array of disks. When the full backup of your data is complete, the disks are transported back to Datastring's Data Center. Future backups, which are purely incremental (incremental forever), will be transmitted via the WAN and synchronized with your initial backup data at the Data Center.

3.4 Do we need to create a user for Datastring on all our servers?

No, but a dedicated user is recommended and it should be set for no password expiration or if password expiration policies must be enforced, use the DS-Client's Password Rotation feature. In a domain, or NDS environment, a user on each machine isn't necessary as one central user can be created with access to all the resources that require backing up.

3.5 Is the Database on the DS-Client backed up?

Yes, by default the DS-Client backs up its own database at 6:00am every morning, although this time can be changed, if desired.

3.6 What happens if too much data is passed to the DS-Client?

The DS-Client only requests data as it can process it and will not pull more data across the network than can be processed. The data sits in a queue and as soon as part of the queue frees up, the DS-Client gets more data for processing

3.7 What is data de-duplication?

De-duplication is one of the ways that the DS-Client reduces the raw data from your network servers across all remote offices to a size that can be transmitted over the WAN. It ensures that the same data is never transmitted offsite more than once, thereby saving the bandwidth to transmit only new, unique data. It achieves this simple elimination by generating a digital signature of each file as it is backed up and comparing it against the known details of all previous files. If the digital signature matches a previously backed up file, it must be a duplicate and only a shortcut need be transmitted up the line. Due to the way this technique is applied, it does not matter if the files are on different servers, at different offices or even have different filenames.

3.8 Can multiple machines be backed up simultaneously?

Delta blocking is a technique that divides all files into blocks. When the file is detected to have changed, the digital signature of each block is compared against the last known digital signature for the same block of the same file (stored in the database on the DS-Client. Any blocks that are different are pulled out to be re- transmitted. These delta blocks will also be compressed and encrypted before transmission.

3.9 What happens if a server stops or crashes during backup or if the backup is interrupted for some other reason?

If the backup is stopped, for whatever reason, it will retry the operation based on the configuration of the DS-Client. If all retries fail it will continue onto the next backup in its schedule. It will not revisit the failed backup set until the next time it is set to run, e.g. the following night, at which point it will pick up where it left off. If however the problem has been rectified and the backup window allows, the backup can be restarted manually, immediately. However, if the backup set is configured with local storage cache the backup will continue its operation by backing up the data locally to the configured buffer.

3.10 Does the DS-Client hold a connection open to aserver all the time?

No, unless CDP is configured the DS-Client will only connect to your servers during the specified backup schedule, therefore it will not use valuable connection at other times.

3.11 How many versions of my backed up files are held offsite?

The number of versions is a parameter that the system administrator can set. Unlike a tape backup, where the routine is to rotate tapes in a cycle, Datastring will only back up a new version of a file when it changes, guaranteeing that the customer is not wasting space backing up exactly the same version more than once. The number of versions stored can be configured on an individual backup item basis. By default, each backup item stores 30 versions, if applicable. Each backup set can be configured down to include just one file if desired, giving you the ability to maximize the efficiency of the storage.

3.12 What platforms are supported? Datastring offers Agentless support for a range of network platforms.

- Extensive OS Support: Windows 2008, Windows 7, Vista, NT, 2000, XP, 2003, Mac OS X, XenSource, VMware, Novell Netware, IBM AIX, SUN Solaris, HP-UX, HP-Tru64 UNIX, IBM iSeries, Red Hat Linux, Novell Suse Linux, etc...

- Extensive Database/Application Support: MS SQL Server, MS Exchange Server & Outlook 2000/2003/ 2007, Oracle, IBM DB2, MySQL, PostgreSQL, IBM Lotus Notes/Domino Server, Novell Groupwise, SAP, MS SharePoint

For more details, see Installation and Backup and Restore Support Matrix for the current version of the software.

3.13 Can the software backup Permissions on files?

Yes, Datastring can backup local/NFS/SSH supporting Unix permissions, POSIX file names and soft links. Also, for NTFS volumes Datastring can backup both permissions and Alternate Data Streams. Permissions and Extended Netware Attributes can also be backed up for Netware.

3.14 If the software is agentless, how are databases such as MS SQL and Exchange backed up?

Microsoft developed SQL and Exchange with the backup requirement in mind. Both products can respond to API calls requesting the services to dump their data, while online, to an external destination. In Datastring's case the product simply asks the specified MS SQL or Exchange server to stream the data to the DS- Client where it is delta blocked and transmitted offsite. This process is a totally supported Microsoft function and guarantees compatibility with your existing Microsoft systems.

3.15 Can Datastring run pre and post commands on servers?

Yes, even though Datastring is an agentless solution, it is still capable of running commands on remote servers. For example, shutting down a database or application running on a server to back it up and restart afterwards, or perhaps interact with some overnight batch processing.

3.16 How does Datastring handle open files?

Open files are an issue in most backup environments. If a file is open exclusively on a workstation, it is the server's responsibility to stop anyone else, including a backup application, accessing that file. To help counteract these issues Datastring has a range of options which handle open files. These options, combined with use of the Pre and Post commands, enable the backup of almost any file. Datastring also can use Microsoft VSS which handles access to open files. More complex environments such as Oracle or DB2 can usually be configured to dump their data into a normal file which will be delta blocked and backed up as normal unless the specific Backup Set type is not used.

3.17 How does datastring handle time zones?

DS-Client and Datastring DS-System run using the time zone set on the machine clock.

3.18 Does a drive defrag negatively affect deduplication?

datastring performs block-level deduplication on files. File system maintenance tasks do not affect files at the level in which datastring influences them. Disk defragmentation will not negatively affect deduplication in any way.

3.19 What happens if the machine the DS- Client resides on fails?

First you need to install an operating system on new or repaired hardware. Then, Datastring will assist you re-installing the DS-Client with the same encryption keys and the same ac- count/DS-Client numbers and recover DS-Client DBs from Se- curStore DS-System. DS-Client can however be installed as grid, thus offering redundancy in case of failures.

3.20 Is it possible to change DS-Client features once it has already been installed ?

Yes. This is accomplished through reconfiguring the parameters on datastring DS-System. In this case Datastring should be contacted to perform the operation.

3.21 Can DS-Client run on Fedora Linux?

No, the DS-Client is not supported running on Fedora Linux. The Linux versions the DS-Client is supported on are RedHat and SUSE.

3.22 How do I specify a "Solaris" backup?

Using the Linux DS-Client, in the New Backup Set Wizard, select Local File System, NFS, UNIX-SSH. There are no specific backup types for different versions of Unix or Linux.

3.23 Is datastring able to backup Exchange cluster through just the passive node?

Yes. There is a feature available in the MS Exchange Database Backup Sets that allows backup of the MS Exchange DB clus- ters using passive node. This option can be found in the New Backup Set Wizard and is simply a checkbox.

3.24 When my DS-Client connects to the Secur Store DS-System, does it come through as the LAN IP of the DS-Client or my Public IP?

ThePublicIP.TheDS-ClientestablishesaTCPconnectiontothe datastring DS-System IP Address provided or DNS name.

3.25 Can Oracle be used as the DS-Client database?

No. Windows DS-Client supports Microsoft SQL Server database instances and Linux DS-Client supports PostgreSQL as the back end database.

3.26 Can the content of any notification email be changed?

The content of notification emails cannot be modified. The subject of notification emails can be changed.

3.27 Datastring support third party open file managers when VSS is not available?

Yes, Datastring does integrate with third party open file managers like St. Bernard OFM.

Monitoring

4.1 How do we control and monitor Datastring?

During installation the DS-User is installed on as many or as few workstations as required and will require a valid logon, en- suring no unauthorized access. The DS-User GUI acts as your interface with datastring and enables the configuration of all backups and restores. The DS-Client Monitoring module can also be used to monitor the activities on the DS-Client.

4.2 How does the Web Portal module help monitor backup sets?

The Web Portal module provides a web point of entry for moni- toring client backups. It stores client account and configura- tion information as well as Web Portal logs. Datastring can set up the web portal so each customer is associated with a unique datastring DS-System IP address or DNS. Web Portal shows the last backup time and the comple- tion (suc- cessful, with errors, premature) for each backup set through its reports. If a backup set completes with errors, the number of errors are shown. A variety of reports can be generated to statistically re- view backup (the number and duration of their connections, number of activities, number of files, protected size etc.) and restore (number of activities, number of files, over a specified period) activities. The Web Portal can also be used to search and download archive data from BLM Archivers.

Compression, Encryption and Security

5.1 Why is encryption done?

DS-Client performs compression and encryption before send-ing data to datastring Data Center.

This ensures security because:

- Data can be restored only by the DS-Client that backed it up, or by another DS-Client that was installed using the same encryption types and keys as the DS-Client that backed up the data.
- Someone monitoring data being transmitted between DS Client and Datastring's Data Center would intercept only encrypted data blocks. This ensures that access to con- fidential file content is not possible.
- Data stored is also encrypted in the Datastring's Data Center. Meaning that only the customer can have access to the backed up data once it has been recovered. The cus- tomer is the only person who knows his/her unique encryption keys.

5.2 To what standard is data encrypted?

datastring's encryption is FIPS 140-2 certified. FIPS certi- fication is given through the Cryptographic Module Validation Program (CMVP) that was established by NIST (National Insti- tute of Standards and Technology) and the Communications Security Establishment (CSE) of the Government of Canada. Products validated as conforming to FIPS 140-2 are accepted by the Federal agencies of both countries (Canada and U.S) for the protection of sensitive information.

5.3 What do you mean by compression? What hap- pens?

Compression can be likened to letting the air out of a balloon. Although the air has gone, the structure still exists and it can be re-inflated easily. The advantage is that it takes less room. Files, especially databases, are often full of empty space, which can be removed to make the file smaller for transit, whilst mak- ing it very easy to recreate. A conservative compression to ex- pect with datastring is 3:1 for the initial backup.

5.4 Why is data compressed?

Compression reduces the amount of data transmitted to the Datastring's Data Center, making backups faster, as well as reducing storage space. Compression is particularly useful for slow communication links and/or very large files.

5.5 Is there added compression on already compressed files (e.g. zip files)?

Zip files and other compressed files are already efficiently com- pressed. datastring cannot improve on the compression, but the file will only be transmitted once. If the file should change, then delta blocking will be used to ensure only the changed portions of the file are re-transmitted. By default Se- curStore will not perform compression on files that are al- ready compressed.

Transmission Off-Site

6.1 Is a WAN connection secure?

The datastring service utilizes a WAN to transmit data offsite. All backup data is compressed,de-duplicated and en- crypted prior to transmission. datastring encryption is FIPS 140-2 certified. Additionally, all communication between datastring software is encrypted with a random encryp- tion key. This is infinitely more secure than many current back- up policies, e.g. 3rd party couriers taking tapes offsite, onsite storage where tapes are left in cupboards overnight.

6.2 What happens if the communication line breaks?

As part of the datastring solution, software will automati- cally attempt to reconnect three times at five minute intervals and will continue the backup process at the block level when the communication line is re- established.

6.3 Does all of our data get transferred every time a backup is scheduled?

Only new and unique data will get backed up after the initial backup. Duplicate or unchanged files will not be transmitted.

6.4 At what point is the data deemed to be backed up offsite?

The data is backed up in real time, so when the administration console indicates that
the backup is complete
- it is also an indication that the backup data is offsite.

6.5 During the backup process are bandwidth notifications available?

DS-Client can be configured to send notifications if a backup set completes successfully, completes with errors or does not complete. Notifications can be sent via SNMP traps or email no- tifications. datastring do have a bandwidth throttle which can be scheduled for certain times of the day. However, there is not an alert available to notify if band- width usage exceeds some threshold. Use the bandwidth throttle functionality to cap to that threshold.

Offsite Storage at Datastring

7.1 Is the backup data held on disk or tape off site?

datastring is a disk to disk solution where data is held on disk for rapid access times and is additionally replicated to an alternate location.

7.2 Is backup data secure and separate from other customers' data?

Yes. Authentication is performed between the relevant DS- Client and system unit each time they connect to re-verify the authenticity of the DS-Client. Additionally, the backup data is held encrypted. Only the customers' unique encryp- tion keys will decrypt the data.

Restoring Data

8.1 At what point is the data available for restore?

The data is available for restore immediately after it has been backed up and is confirmed to be held offsite.

8.2 Can an individual file be restored?

Yes, you can restore an individual file and also specify which version you want to restore.

8.3 How does datastring handle message level restores for emails?

The Message Level Restore (MLR) module allows users to se- lectively backup and restore individual mailboxes and email messages for one user or for an entire email server, depend- ing on needs. Using selective filtering, users can save time and resources by restor- ing only selected mailboxes or emails, instead of having to re- store the entire Exchange, Domino or GroupWise servers.

8.4 Can you restore a whole backup set to a point in time, e.g. last Monday?

Yes, datastring will display all the files that were backed up on any given day. Providing the backed up files have not been deleted by an administrator or overwritten by more re- cent versions, then it is possible to restore up to any given date.

8.5 8.5 Can data be restored to a different machine on our network?

Yes, the restore data can be redirected as desired. You are able to browse the network and provide connection credentials for the redirected restore location, just as you do for creating the backup set.

Disaster Recovery

9.1 Can we prioritize which data is restored in the event of a disaster?

Yes, you can select easily which files/directories/servers you wish to restore. There is no need to restore non-essential data until a later time if desired.

9.2 What happens if the DS-Client and/or the whole site is lost?

datastring can interact closely with your disaster recov- ery and business continuity plan, providing a portable unit of disks, holding your data and a new DS-Client to any required site. This site may even be the site of your disaster recovery company. This combination of portable unit and new DS-Cli- ent can enable LAN speed restores to recon- struct servers and workstations.

9.3 Can we perform a test re-build of the DS-Cli ent and restore data?

Yes, Disaster Recovery drills can be performed periodically if requested.

Local Storage

10.1 Is it possible to have a copy of the backed up data locally on DS-Client LAN?

DS-Client can be configured to store up to the last 30 days of backup locally to the DS-Client LAN in compressed format. This storage option is in addition to keep the data on the Secur- Store DS-System and provides option for fast local restores of large data sets in case of disasters and recoverability of data in the event that the datastring DS-System is unavailable.

Data Protection

11.1 Can datastring backup laptops?

Absolutely. datastring software can backup laptops with our DS-Mobile Client application that has a small footprint, CPU and bandwidth throttle and secure, efficient transmis- sion of data or with the datastring DS-Client.

11.2 How do I backup a NetApp appliance?

A NetApp appliance is backed up the same way as any other NAS device. You do so by backing up the data through exported shares (i.e. CIFS shares for Windows, NFS shares for Linux).

11.3 What is LAN Discovery?

LAN Discovery is a tool used to discover data within a network that can be protected with a DS-Client in that location. LAN Discovery allows the datastring to generate reports about data volume, location, duplicate data, access trends and storage space.

11.4 Why is a statistical backup useful?

Statistical-mode backup is a method that performs a “dry run” on a backup set. This process performs 100% of the function- ality of a regular backup with the exception of sending data to the datastring DS- System. Actual dedupli- cation and compression statistics are generated along with information regarding the amount of net-new data created and backup set completion time. With all of the information contained in reports after running a statistical backup, datastring can give a customer a real-world costing and performance estimate.

Virtualization

12.1 How does datastring protect ESX servers?

datastring uses the Linux datastring DS-Client to perform backup and recovery of virtual machines at the VM-level. The datastring DS-Client interfaces agentlessly with ESX server or Virtual Center to perform backup without the need for any other 3rd party products. Recovery can be performed to any ESX server.

12.2 Can DS-Client run on a virtual machine?

Yes. DS-Client can run on Windows, Red Hat or SUSE native or virtual machines.

12.3 If I backup both VMWare ESX host side and guest OS side, will files that are backed up from the guest side be de-duplicated when you backup the VMDK file from the host side?

datastring de-duplicates at the block level. Since all the guest OS files appear as one large VMDK file from the host side, individual files backed up from the guest side will not be de-duplicated within the VMDK file. However, if the same file was stored in multiple different directories on the guest side, these would appear as repeating blocks within the VMDK file and these blocks would be de-duplicated.

12.4 Can I backup VMWare environment with a windows DS-Client?

If you want to backup the VM from the host side (i.e. backup the VMDK and associated files), you must use the Linux DS-Client. However, a Windows DS-Client can backup and restore Windows Virtual Machines through the guest Windows operating system. A Windows DS-Client can also be used to backup and restore via VMWare Consolidated Backup and File System Backup Sets.

12.5 I want to backup the same VMguests via VMDK and system/file level. If I backup a VMDK, and the same system via file level, that has for example ~100 Word docs, will the VMDK dedupe against the file level backup or just against the other VMDK?

VMDK refers to extension of the files that implement virtual machines. Thus, the VMDK is normally a single file (depending on configuration a VMDK can also be split into chunks) and looks for duplicate VMDK files. It is doubtful that any two VMDK files will be identical. Therefore, VMDK will not dedupe against files backed up from the guest. The incremental VMDK backups will only backup the blocks that change within the VMDK file.

12.6 Is datastring capable of restoring one file within an ESX without restoring the entire guest?

Yes. However, VM-level backups of ESX hosts are recommended for DR purposes and whole machine recoverability. File-level backup sets may be necessary to meet the most granular restoration requirements. Often a hybrid approach of both VM-level and file-level specific backups makes sense.